(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－114806
（P2003－114806A）
(43)公開日　平成15年４月18日(2003.4.18)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　11/00		Ｇ０６Ｆ	9/06	６３０Ａ　５Ｂ０７６

審査請求　未請求　請求項の数10　ＯＬ　（全 13 頁）

(21)出願番号　特願2001－308156(P2001－308156)

(22)出願日　平成13年10月４日(2001.10.4)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　大島　剛
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　木村　信二
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

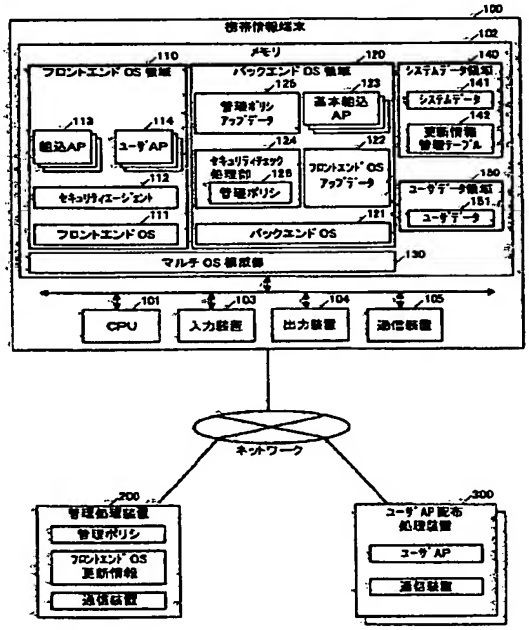
(74)代理人　100083552
弁理士　秋田　収喜

最終頁に続く

(54)【発明の名称】　ＯＳ更新方法及びセキュリティ制御方法並びにその実施装置

(57)【要約】
【課題】　情報処理装置のＯＳの更新を効率良く行うことが可能な技術を提供する。
【解決手段】　情報処理装置内にインストールされているＯＳを更新するＯＳ更新方法において、通常のアプリケーション処理を制御するフロントエンドＯＳの更新が必要であるかどうかを判定するステップと、前記フロントエンドＯＳの更新が必要であると判定された場合に、動作中のフロントエンドＯＳの処理を終了させて情報処理装置の制御をバックエンドＯＳに切り換えるステップと、フロントエンドＯＳを最新の状態に更新する為の更新データをバックエンドＯＳの制御下で取得してフロントエンドＯＳを最新の状態に更新するステップと、前記最新の状態に更新されたフロントエンドＯＳを再起動するステップとを有するものである。

図１



1

【特許請求の範囲】

【請求項１】　情報処理装置内にインストールされているＯＳを更新するＯＳ更新方法において、

通常のアプリケーション処理を制御するフロントエンドＯＳの更新が必要であるかどうかを判定するステップと、前記フロントエンドＯＳの更新が必要であると判定された場合に、動作中のフロントエンドＯＳの処理を終了させて情報処理装置の制御をバックエンドＯＳに切り換えるステップと、フロントエンドＯＳを最新の状態に更新する為の更新データをバックエンドＯＳの制御下で取得してフロントエンドＯＳを最新の状態に更新するステップと、前記最新の状態に更新されたフロントエンドＯＳを再起動するステップとを有することを特徴とするＯＳ更新方法。

【請求項２】　フロントエンドＯＳの制御下で取得または作成されたデータをフロントエンドＯＳの格納領域とは異なる領域に格納し、更新前のフロントエンドＯＳの制御下で取得または作成されたデータを更新後のフロントエンドＯＳの制御下で再利用することを特徴とする請求項１に記載されたＯＳ更新方法。

【請求項３】　前記切り換えられたバックエンドＯＳの制御下で必要最小限のアプリケーション処理を実行することを特徴とする請求項１または請求項２のいずれかに記載されたＯＳ更新方法。

【請求項４】　情報処理装置内で実行されるアプリケーション処理のセキュリティを制御するセキュリティ制御方法において、

情報処理装置上でアプリケーションの処理要求が行われた場合に、その処理要求が許可されているかどうかの問合せを行うステップと、前記問合せの行われた処理要求が許可されているかどうかを管理ポリシに従って判定した後、その判定内容を示す問合せ結果を応答するステップと、前記問合せ結果の内容が当該アプリケーション処理の実行許可を示している場合にそのアプリケーション処理を実行するステップとを有することを特徴とするセキュリティ制御方法。

【請求項５】　アプリケーションの処理要求が行われたＯＳとは異なるＯＳの制御下で前記管理ポリシを管理することを特徴とする請求項４に記載されたセキュリティ制御方法。

【請求項６】　管理処理装置内に格納された管理ポリシの内容に従って情報処理装置内の管理ポリシを更新することを特徴とする請求項４または請求項５のいずれかに記載されたセキュリティ制御方法。

【請求項７】　前記問合せは、当該アプリケーションプログラムの実行可否、当該アプリケーションによる端末内の情報へのアクセス可否、外部との通信可否を問合せるものであることを特徴とする請求項４乃至請求項６のいずれか１項に記載されたセキュリティ制御方法。

【請求項８】　装置内にインストールされているＯＳを

2

更新する情報処理装置において、

通常のアプリケーション処理を制御するフロントエンドＯＳの更新が必要であるかどうかを判定し、フロントエンドＯＳを最新の状態に更新する為の更新データをバックエンドＯＳの制御下で取得してフロントエンドＯＳを最新の状態に更新するフロントエンドＯＳアップデータと、

前記フロントエンドＯＳの更新が必要であると判定された場合に、動作中のフロントエンドＯＳの処理を終了させて情報処理装置の制御をバックエンドＯＳに切り換えた後、前記最新の状態に更新されたフロントエンドＯＳを再起動するマルチＯＳ構成部とを備えることを特徴とする情報処理装置。

【請求項９】　装置内で実行されるアプリケーション処理のセキュリティを制御する情報処理装置において、

情報処理装置上でアプリケーションの処理要求が行われた場合に、その処理要求が許可されているかどうかの問合せをセキュリティチェック処理部に送り、前記問合せ結果の内容が当該アプリケーション処理の実行許可を示している場合にそのアプリケーション処理を実行するセキュリティエージェントと、

前記問合せの行われた処理要求が許可されているかどうかを管理ポリシに従って判定した後、その判定内容を示す問合せ結果をセキュリティエージェントに応答するセキュリティチェック処理部とを備えることを特徴とする情報処理装置。

【請求項１０】　管理処理装置内に格納された管理ポリシの内容に従って情報処理装置内の管理ポリシを更新する管理ポリシアップデータを備えることを特徴とする請求項９に記載された情報処理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はオペレーティングシステム（ＯＳ）の更新、管理ポリシに従ったセキュリティの実現及び管理ポリシのリモートメンテナンスを行う情報処理装置に関し、特にＯＳの更新機能、セキュリティ機能及びリモートメンテナンス機能を複数のＯＳの搭載により提供する情報処理装置に適用して有効な技術に関するものである。

【０００２】

【従来の技術】近年の携帯電話等の携帯情報端末の急速な進歩に伴い、インターネットにアクセスしたり、音楽データをダウンロードして再生したり、利用者の写真を撮影して電子メールとして送信する等、携帯情報端末によって様々な機能が提供される様になってきている。

【０００３】この様な携帯情報端末では、携帯情報端末内の不揮発性メモリにＯＳ、組込アプリケーションプログラム（組込ＡＰ）及びユーザアプリケーションプログラム（ユーザＡＰ）やそれらの処理でアクセスされるデータを格納しておき、電源投入時や利用者からの操作が

行われたときに前記不揮発性メモリ上のプログラムを起動して各種機能を提供している。

【０００４】前記従来の携帯情報端末において、新たに機能追加を行う場合や既存のプログラムの修正を行う場合には前記不揮発性メモリ上のプログラムを更新する必要があるが、携帯情報端末内の不揮発性メモリ上のプログラムを更新する場合、携帯情報端末をパーソナルコンピュータ（ＰＣ）等の専用の情報処理装置に接続し、その情報処理装置の動作によって携帯情報端末内の不揮発性メモリの内容を書き換える必要があり、一般のユーザが行うのは困難である為、端末本体をサービスセンタに持ち込んでプログラムの書き換えを行っている。またその際の費用は端末提供者によって負担されている。

【０００５】一方、高性能化、多機能化する携帯情報端末では、ユーザＡＰをダウンロードして実行できる携帯情報端末が増えているが、アプリケーション処理の実行の際に携帯情報端末内にある情報にアクセスできるかどうかや、外部との通信を行えるかどうかといったセキュリティに関する設定は、その携帯情報端末を提供しているサービス事業者側によって全て行われている。

【０００６】例えば、一般消費者向けのサービスを行っているサービス事業者は、端末内の住所録が外部に漏れることを防ぐ為、端末内の情報と外部に同時にアクセスできるアプリケーションを、サービス事業者自らが提供するアプリケーションだけに制限している。

【０００７】なお、フラッシュメモリに記憶された、複数のプログラムブロックからなるプログラムデータの一部のプログラムブロックのデータを更新するプログラム更新装置およびプログラム更新方法については、特開２０００－２４２４８７号公報に記載されている。その概要は、Ａ～Ｅの各機能を実現するための複数のプログラムブロックを記憶したフラッシュメモリに対して、たとえば、機能ＤのＯＳデータを更新する場合、第４番目のメモリブロックのデータを消去する前に、機能ＤのＯＳデータとともに第４番目のメモリブロック内に格納された、機能ＣのＯＳデータの一部と機能ＥのＯＳデータの一部のデータを、パーソナルコンピュータに一時的に退避し、第４番目のメモリブロックのデータを消去した後、新しい機能ＤのＯＳデータとともに退避データを第４番目のメモリブロックの元の位置に書き込むものである。

【０００８】

【発明が解決しようとする課題】前記従来の携帯情報端末では、ＯＳや組込ＡＰ等の更新を利用者側で行うことが困難であり、端末本体をサービスセンタに持ち込んでプログラムの書き換えを行う必要がある為、ＯＳや組込ＡＰの更新作業に多大な時間と莫大な費用を要するという問題がある。今後、携帯情報端末の高機能化、高性能化に伴って、バグの発生という問題は益々多くなると考えられる為、このプログラムの更新時の問題を解決する必要がある。

【０００９】一方、高性能化、多機能化する携帯情報端末では、今後、現在のＰＣの様にビジネスの世界に進出することが予想されるが、現状の携帯情報端末のセキュリティは、その携帯情報端末を提供しているサービス事業者側で全て設定されている為、企業がこれを利用する場合、自分たちが設定した業務用のアプリケーションも端末内外の情報にアクセスできる様にする等のサービス事業者とは異なる基準でアプリケーションのアクセス可否を決定することができないという問題がある。

【００１０】また、前記従来の携帯情報端末において、サービス事業者が企業側の要求に沿ってアクセス可否の情報を設定したとしても、一旦設定されたアプリケーションのアクセス可否の様な情報は端末内の不揮発性メモリに記憶されており、この情報を更新するリモートメンテナンス等の有効な手段が提供されていない為、業務内容の変化に応じて業務用アプリケーションの機能を変更する度に端末を回収して、専用の装置を使って業務用アプリケーション及び対応するセキュリティ情報を更新する必要があり、業務用アプリケーション及びそのセキュリティ情報のメンテナンスに大きな時間と費用がかかるという問題がある。

【００１１】本発明の目的は上記問題を解決し、情報処理装置のＯＳの更新を効率良く行うことが可能な技術を提供することにある。本発明の他の目的は情報処理装置で利用者独自の基準に基づいたセキュリティ機能を実現することが可能な技術を提供することにある。本発明の他の目的は情報処理装置内のセキュリティ機能をリモートメンテナンスすることが可能な技術を提供することにある。

【００１２】

【課題を解決するための手段】本発明は、装置内にインストールされているＯＳを更新する情報処理装置において、フロントエンドＯＳの更新が必要であると判定された場合にバックエンドＯＳの制御下でフロントエンドＯＳの更新を行うものである。

【００１３】本発明では、携帯電話等の携帯情報端末である情報処理装置からネットワークを介して管理処理装置へアクセスし、通常のアプリケーション処理を制御するフロントエンドＯＳの更新情報を管理処理装置から取得して、情報処理装置内にインストールされているフロントエンドＯＳの管理情報と前記取得した更新情報とを比較し、情報処理装置内にインストールされているフロントエンドＯＳの更新が必要であるかどうかを判定する。

【００１４】前記フロントエンドＯＳの更新が必要であると判定された場合には、マルチＯＳ構成部の処理により、動作中のフロントエンドＯＳの処理を終了させて情報処理装置内の各部の制御をバックエンドＯＳに切り換えることによってバックエンドＯＳの制御下での情報処

理装置の動作を可能とした後、ネットワークを介して管理処理装置へアクセスし、フロントエンドＯＳを最新の状態に更新する為の更新データをバックエンドＯＳの制御下で管理処理装置から取得してフロントエンドＯＳを最新の状態に更新する。

【００１５】そして、前記最新の状態に更新されたフロントエンドＯＳを再起動した後、情報処理装置内の各部の制御を更新後のフロントエンドＯＳに切り換えて、更新後のフロントエンドＯＳの制御による情報処理装置の動作を可能とする。

【００１６】以上の様に本発明の情報処理装置によれば、フロントエンドＯＳの更新が必要であると判定された場合にバックエンドＯＳの制御下でフロントエンドＯＳの更新を行うので、情報処理装置のＯＳの更新を効率良く行うことが可能である。

【００１７】

【発明の実施の形態】以下にＯＳの更新機能、セキュリティ機能及びリモートメンテナンス機能を複数のＯＳの搭載により提供する一実施形態の情報処理装置について説明する。

【００１８】図１は本実施形態の携帯情報端末マルチＯＳシステムの概略構成を示す図である。図１に示す様に本実施形態の携帯情報端末マルチＯＳシステムは、携帯情報端末１００と、管理処理装置２００と、ユーザＡＰ配布処理装置３００とを有している。

【００１９】携帯情報端末１００は、管理処理装置２００からフロントエンドＯＳ更新情報や管理ポリシを取得し、ＯＳの更新機能、セキュリティ機能及びリモートメンテナンス機能を実現する携帯電話等の携帯型の情報処理装置である。

【００２０】管理処理装置２００は、フロントエンドＯＳ更新情報や管理ポリシについて、それらの最新情報を携帯情報端末１００へ提供する処理装置である。ユーザＡＰ配布処理装置３００は、携帯情報端末１００からの要求に応じてユーザＡＰを携帯情報端末１００へ配布する処理装置である。

【００２１】携帯情報端末１００は、ＣＰＵ１０１と、メモリ１０２と、入力装置１０３と、出力装置１０４と、通信装置１０５と、フロントエンドＯＳ領域１１０と、バックエンドＯＳ領域１２０と、管理ポリシ１２６と、システムデータ領域１４０と、システムデータ１４１と、更新情報管理テーブル１４２と、ユーザデータ領域１５０と、ユーザデータ１５１とを有している。

【００２２】ＣＰＵ１０１は、携帯情報端末１００全体の動作を制御する装置である。メモリ１０２は、携帯情報端末１００全体の動作を制御する際にその為の各種処理プログラムやデータをロードするフラッシュメモリ等の不揮発性の記憶装置である。

【００２３】入力装置１０３は、携帯情報端末１００を操作する為の各種入力を行う装置である。出力装置１０４は、携帯情報端末１００の操作に伴う各種出力を行う装置である。通信装置１０５は、インターネットやイントラネット等のネットワークを介して他の処理装置との通信を行うと共に音声通話も行う装置である。

【００２４】フロントエンドＯＳ領域１１０は、フロントエンドＯＳ１１１及びその制御下で動作する各種プログラムを格納する領域である。バックエンドＯＳ領域１２０は、バックエンドＯＳ１２１及びその制御下で動作する各種プログラムを格納する領域である。管理ポリシ１２６は、携帯情報端末１００上で実行が許可されているアプリケーション処理の内容を示すデータである。

【００２５】システムデータ領域１４０は、システムデータ１４１を格納する領域である。システムデータ１４１は、フロントエンドＯＳ１１１、バックエンドＯＳ１２１及びマルチＯＳ構成部１３０等のシステムプログラムが動作する際に用いられるデータである。更新情報管理テーブル１４２は、フロントエンドＯＳ１１１及び組込ＡＰ１１３の更新情報を格納するテーブルである。

【００２６】ユーザデータ領域１５０は、ユーザデータ１５１を格納する領域である。ユーザデータ１５１は、ユーザＡＰ１１４等のアプリケーション処理で取得または作成された住所録データや予定表データ等のデータである。

【００２７】また携帯情報端末１００は、フロントエンドＯＳ１１１と、セキュリティエージェント１１２と、組込ＡＰ１１３と、ユーザＡＰ１１４と、バックエンドＯＳ１２１と、フロントエンドＯＳアップデータ１２２と、基本組込ＡＰ１２３と、セキュリティチェック処理部１２４と、管理ポリシアップデータ１２５と、マルチＯＳ構成部１３０とを有している。

【００２８】フロントエンドＯＳ１１１は、組込ＡＰ１１３やユーザＡＰ１１４等の通常のアプリケーション処理を制御するＯＳである。セキュリティエージェント１１２は、携帯情報端末１００上でアプリケーションの処理要求が行われた場合に、その処理要求が許可されているかどうかの問合せをセキュリティチェック処理部１２４に送り、前記問合せ結果の内容が当該アプリケーション処理の実行許可を示している場合にそのアプリケーション処理を実行する処理部である。

【００２９】組込ＡＰ１１３は、フロントエンドＯＳ１１１に組み込まれた住所録編集処理等の所定のアプリケーション処理を実行する処理部である。ユーザＡＰ１１４は、ユーザＡＰ配布処理装置３００から配布された見積処理等の所定のアプリケーション処理を実行する処理部である。

【００３０】バックエンドＯＳ１２１は、フロントエンドＯＳ１１１の停止中に携帯情報端末１００の動作を制御し、セキュリティチェック処理の際、セキュリティエージェント１１２からの処理要求に答えて動作するＯＳである。

7

【００３１】フロントエンドＯＳアップデータ１２２は、通常のアプリケーション処理を制御するフロントエンドＯＳ１１１の更新が必要であるかどうかを判定し、フロントエンドＯＳ１１１を最新の状態に更新する為の更新データをバックエンドＯＳ１２１の制御下で取得してフロントエンドＯＳ１１１を最新の状態に更新する処理部である。

【００３２】基本組込ＡＰ１２３は、組込ＡＰ１１３の中で携帯電話として動作する為の必要最低限のサブセットであり、例えば組込ＡＰ１１３に住所録ＡＰ、着メロ作成ＡＰ、ゲームＡＰがあった場合、閲覧とそれによる電話のみが行える住所録ＡＰだけが入っており、バックエンドＯＳ１２１側にバグが入り込む余地をなるべく少なくした処理部である。

【００３３】セキュリティチェック処理部１２４は、前記問合せの行われた処理要求が許可されているかどうかを管理ポリシ１２６に従って判定した後、その判定内容を示す問合せ結果をセキュリティエージェント１１２に応答する処理部である。管理ポリシアップデータ１２５は、管理処理装置２００内に格納された管理ポリシの内容に従って携帯情報端末１００内の管理ポリシ１２６を更新する処理部である。

【００３４】マルチＯＳ構成部１３０は、フロントエンドＯＳ１１１及びバックエンドＯＳ１２１をタイムスライスで動作させてフロントエンドＯＳ１１１上のセキュリティエージェント１１２とバックエンドＯＳ１２１上のセキュリティチェック処理部１２４との間の通信を制御し、フロントエンドＯＳ１１１の更新が必要であると判定された場合に、動作中のフロントエンドＯＳ１１１の処理を終了させて携帯情報端末１００の制御をバックエンドＯＳ１２１に切り換えた後、前記最新の状態に更新されたフロントエンドＯＳ１１１を再起動する処理部である。

【００３５】携帯情報端末１００をフロントエンドＯＳ１１１、セキュリティエージェント１１２、組込ＡＰ１１３、ユーザＡＰ１１４、バックエンドＯＳ１２１、フロントエンドＯＳアップデータ１２２、基本組込ＡＰ１２３、セキュリティチェック処理部１２４、管理ポリシアップデータ１２５及びマルチＯＳ構成部１３０として機能させる為のプログラムは、フラッシュメモリ等の記録媒体に記録されて実行されるものとする。なお前記プログラムを記録する記録媒体はフラッシュメモリ以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【００３６】本実施形態の携帯情報端末１００では、組込ＡＰ１１３やユーザＡＰ１１４等の通常のアプリケーション処理を制御するフロントエンドＯＳ１１１と、フロントエンドＯＳ１１１の停止中に携帯情報端末１００

8

の動作を制御するバックエンドＯＳ１２１とがタイムスライスで動作するマルチＯＳの構成をとっており、フロントエンドＯＳ１１１として優れたＧＵＩ(Graphical User Interface)を備える最新のＯＳをインストールし、バックエンドＯＳ１２１として動作の安定している以前のバージョンのＯＳを用いて携帯情報端末１００を動作させているものとする。ここで、バックエンドＯＳ１２１として、安定動作することが判っている別のＯＳを使ったり、同じバージョンでも機能を大きく制限することによって安定させたＯＳを用いても良い。

【００３７】フロントエンドＯＳ１１１に新しい機能を追加する場合や、フロントエンドＯＳ１１１の新たに発見された不具合を修正する場合には、マルチＯＳ構成部１３０により携帯情報端末１００の入力装置１０３、出力装置１０４及び通信装置１０５を、フロントエンドＯＳ１１１からバックエンドＯＳ１２１に割り当てて動作させ、バックエンドＯＳ１２１の制御下でフロントエンドＯＳ１１１の更新を行う。ここで、マルチＯＳ構成部１３０によるフロントエンドＯＳ１１１からバックエンドＯＳ１２１への切り替えは、フロントエンドＯＳ１１１にマッピングされていたＩ／Ｏ処理の割り込みをバックエンドＯＳ１２１にマッピングすることにより行うものとする。

【００３８】以下に本実施形態の携帯情報端末マルチＯＳシステムにおいて、バックエンドＯＳ１２１の制御下でフロントエンドＯＳアップデータ１２２を動作させ、ネットワークを介して更新データをダウンロードして更新処理を実行し、フロントエンドＯＳ１１１及び組込ＡＰ１１３を更新する処理について説明する。

【００３９】図２は本実施形態のフロントエンドＯＳアップデータ１２２の処理手順を示すフローチャートである。図２に示す様に本実施形態の携帯情報端末１００のフロントエンドＯＳアップデータ１２２は、通常のアプリケーション処理を制御するフロントエンドＯＳ１１１の更新が必要であるかどうかを判定し、フロントエンドＯＳ１１１を最新の状態に更新する為の更新データをバックエンドＯＳ１２１の制御下で取得してフロントエンドＯＳ１１１を最新の状態に更新する処理を行う。

【００４０】ステップ２０１で携帯情報端末１００のフロントエンドＯＳアップデータ１２２は、前回の処理からの所定時間の経過や利用者から特定のキーが押された場合等、フロントエンドＯＳ１１１の更新処理を開始する所定の条件が満たされたかどうかを調べ、前記条件が満たされている場合にはステップ２０２へ進む。

【００４１】ステップ２０２では、携帯情報端末１００にインストールされているフロントエンドＯＳ１１１及び組込ＡＰ１１３の各種情報が格納されている更新情報管理テーブル１４２の内容を読み出す。

【００４２】図３は本実施形態の更新情報管理テーブル１４２の一例を示す図である。図３に示す様に本実施形

態の更新情報管理テーブル１４２には、フロントエンドＯＳ領域１１０に格納されているフロントエンドＯＳ１１１及び組込ＡＰ１１３のバージョン、フロントエンドＯＳ１１１及び組込ＡＰ１１３がフロントエンドＯＳ領域１１０に格納された日付を示す更新日付、フロントエンドＯＳ領域１１０での格納アドレスとその長さ、フロントエンドＯＳ１１１及び組込ＡＰ１１３の更新情報を提供している管理処理装置２００のアドレスを示す更新情報取得先ＵＲＬ(Uniform Resource Locator)が格納されている。

【００４３】ステップ２０３でフロントエンドＯＳアップデータ１２２は、前記読み出した更新情報管理テーブル１４２中の更新情報取得先ＵＲＬに示された管理処理装置２００のアドレスにアクセスし、フロントエンドＯＳ１１１及び組込ＡＰ１１３の更新情報の送信を管理処理装置２００に要求する。

【００４４】この更新情報の要求の際に、通信装置１０５がフロントエンドＯＳ１１１に割り当てられており、バックエンドＯＳ１２１に割り当てられていない場合には、フロントエンドＯＳ１１１からバックエンドＯＳ１２１への通信装置１０５の接続の切り換え要求をマルチＯＳ構成部１３０に対して行うものとする。なおバックエンドＯＳ１２１としてリアルタイム処理に優れたＯＳを採用し、通信処理に関しては常にバックエンドＯＳ１２１が行っているものとしても良い。

【００４５】管理処理装置２００は、フロントエンドＯＳ１１１及び組込ＡＰ１１３の更新情報の取得要求を携帯情報端末１００から受信すると、管理処理装置２００内に格納されているフロントエンドＯＳ更新情報を読み出し、携帯情報端末１００へ送信する。ここで管理処理装置２００のフロントエンドＯＳ更新情報には、最新のフロントエンドＯＳ１１１及び組込ＡＰ１１３のバージョン及び更新日付が格納されているものとする。

【００４６】携帯情報端末１００のフロントエンドＯＳアップデータ１２２は、管理処理装置２００からフロントエンドＯＳ更新情報を受信するとステップ２０４に進み、更新情報管理テーブル１４２中に格納されているフロントエンドＯＳ１１１及び組込ＡＰ１１３のバージョン及び更新日付と、管理処理装置２００から受信したフロントエンドＯＳ更新情報中のバージョン及び更新日付とを比較し、更新情報管理テーブル１４２中に格納されているバージョン及び更新日付の方が古い場合には、更新処理が必要であるものとしてステップ２０５へ進む。

【００４７】ステップ２０５では、バックエンドＯＳ１２１を介してマルチＯＳ構成部１３０を呼び出し、フロントエンドＯＳ１１１及び組込ＡＰ１１３の終了をマルチＯＳ構成部１３０に要求する。

【００４８】マルチＯＳ構成部１３０は、フロントエンドＯＳ１１１及び組込ＡＰ１１３の終了要求をフロントエンドＯＳアップデータ１２２から受け取ると、動作中

のフロントエンドＯＳ１１１及び組込ＡＰ１１３の処理を終了させた後、入力装置１０３、出力装置１０４及び通信装置１０５等のリソースをバックエンドＯＳ１２１に割り当て、携帯情報端末１００の制御をバックエンドＯＳ１２１に切り換える。

【００４９】ここで利用者からアプリケーション処理の実行要求が入力された場合には、バックエンドＯＳ１２１を介して基本組込ＡＰ１２３を動作させることにより、フロントエンドＯＳ１１１の更新中でも必要最小限の処理を行うものとする。

【００５０】またシステムデータ１４１やユーザデータ１５１は、フロントエンドＯＳ領域１１０とは異なるシステムデータ領域１４０やユーザデータ領域１５０に格納されているので、必要最小限の処理を提供するバックエンドＯＳ１２１や基本組込ＡＰ１２３は、フロントエンドＯＳ１１１で用いられていたシステムデータ１４１やユーザデータ１５１をそのまま利用してフロントエンドＯＳ１１１及び組込ＡＰ１１３と同様の処理を利用者に提供することができる。

【００５１】ステップ２０６でフロントエンドＯＳアップデータ１２２は、前記読み出した更新情報管理テーブル１４２中の更新情報取得先ＵＲＬに示された管理処理装置２００のアドレスにアクセスし、フロントエンドＯＳ１１１及び組込ＡＰ１１３を最新の状態に更新する為の更新データの送信を管理処理装置２００に要求する。

【００５２】ここで前記更新データは、フロントエンドＯＳ１１１及び組込ＡＰ１１３を最新の状態に更新する為のインストールプログラムまたは差分データ、或いは最新のフロントエンドＯＳ１１１及び組込ＡＰ１１３そのもののいずれであっても良いものとする。

【００５３】ステップ２０７でフロントエンドＯＳアップデータ１２２は、管理処理装置２００から送信された更新データを受信し、その更新データを用いて、更新情報管理テーブル１４２中の格納アドレス及び長さで示された領域に格納されているフロントエンドＯＳ１１１及び組込ＡＰ１１３を最新の状態に更新した後、更新情報管理テーブル１４２中のバージョン、更新日付等の情報を新しい内容に更新する。

【００５４】ステップ２０８では、バックエンドＯＳ１２１を介してマルチＯＳ構成部１３０を呼び出し、フロントエンドＯＳ１１１及び組込ＡＰ１１３の再起動を指示する。

【００５５】マルチＯＳ構成部１３０は、フロントエンドＯＳ１１１及び組込ＡＰ１１３の再起動指示をフロントエンドＯＳアップデータ１２２から受け取ると、更新後のフロントエンドＯＳ１１１及び組込ＡＰ１１３を再起動させた後、入力装置１０３、出力装置１０４及び通信装置１０５等のリソースをフロントエンドＯＳ１１１に割り当て、携帯情報端末１００の制御をフロントエンドＯＳ１１１に切り換える。

11

【００５６】従来の携帯情報端末では、不揮発性メモリに格納されているＯＳや組込ＡＰを実行させることにより動作している為、ＯＳや組込ＡＰの更新を行う際に更新対象のＯＳや組込ＡＰの動作を停止させる必要があるが、ＯＳを停止させると携帯情報端末単独では動作できなくなる為、端末本体をサービスセンタに持ち込んで専用の装置に接続し、プログラムの書き換えを行う必要があった。

【００５７】これに対し、本実施形態の携帯情報端末マルチＯＳシステムでは、更新対象のフロントエンドＯＳ１１１及び組込ＡＰ１１３を停止させた後、携帯情報端末１００の制御をバックエンドＯＳ１２１に移し、バックエンドＯＳ１２１の制御下でフロントエンドＯＳアップデータ１２２を動作させるので、ネットワークを介して更新データをダウンロードして更新処理を実行し、オンラインでフロントエンドＯＳ１１１及び組込ＡＰ１１３の更新を行うことができる。

【００５８】本実施形態では、ＯＳや組込ＡＰを不揮発性メモリに格納している携帯情報端末１００においてフロントエンドＯＳ１１１及び組込ＡＰ１１３を更新する処理について説明したが、磁気ディスク装置に格納されたＯＳや組込ＡＰをメモリにロードして実行するＰＣ等の情報処理装置に適用しても良い。

【００５９】従来の情報処理装置では、ＣＤ－ＲＯＭ等の可搬型の記録媒体を用い、人手を介してプログラムの更新が行われているが、本実施形態では、ネットワークを介してオンラインで更新処理を行うので、人手を介すること無く更新処理を効率的に行うことが可能である。

【００６０】また従来の情報処理装置では、更新処理用の記録媒体の内容をネットワーク経由で取得してオンラインで更新処理を行うことも考えられるが、ＯＳや組込ＡＰの不具合を修正する目的で更新処理を行う場合、シングルＯＳ環境下では不具合の有るＯＳや組込ＡＰを用いて通信処理を行うことになる為、その不具合により通信処理が正常に実行できず、更新処理を行えない可能性がある。

【００６１】これに対して本実施形態では、不具合のあるフロントエンドＯＳ１１１及び組込ＡＰ１１３を停止し、動作の安定しているバックエンドＯＳ１２１の制御下で更新処理を行うので、更新対象の不具合に影響されること無く更新処理を効率的に行うことが可能である。

【００６２】次に、本実施形態の携帯情報端末マルチＯＳシステムにおいて、バックエンドＯＳ領域１２０中の管理ポリシ１２６に従ったセキュリティ機能を実現する処理について説明する。

【００６３】図４は本実施形態のセキュリティエージェント１１２の処理手順を示すフローチャートである。図４に示す様に本実施形態のセキュリティエージェント１１２は、携帯情報端末１００上でアプリケーションの処理要求が行われた場合に、その処理要求が許可されているかどうかの問合せをセキュリティチェック処理部１２４に送り、前記問合せ結果の内容が当該アプリケーション処理の実行許可を示している場合にそのアプリケーション処理を実行する処理を行う。

12

【００６４】ステップ４０１で携帯情報端末１００のセキュリティエージェント１１２は、携帯情報端末１００上で行われたアプリケーションの処理要求の内容を調べ、その処理要求がアプリケーション処理の起動要求である場合にはステップ４０２へ進む。

【００６５】ステップ４０２では、その起動要求の行われたアプリケーションの名称を指定し、そのアプリケーション処理の実行が許可されているかどうかの問合せを、フロントエンドＯＳ１１１、マルチＯＳ構成部１３０及びバックエンドＯＳ１２１を経由してセキュリティチェック処理部１２４に送る。

【００６６】図５は本実施形態のセキュリティチェック処理部１２４の処理手順を示すフローチャートである。図５に示す様に本実施形態のセキュリティチェック処理部１２４は、セキュリティエージェント１１２から問合せの行われた処理要求が許可されているかどうかを管理ポリシ１２６に従って判定した後、その判定内容を示す問合せ結果をセキュリティエージェント１１２に応答する処理を行う。

【００６７】ステップ５０１で携帯情報端末１００のセキュリティチェック処理部１２４は、セキュリティエージェント１１２からの問合せの内容を調べ、その問合せ内容がアプリケーション処理の実行が許可されているかどうかの問合せである場合にはステップ５０２へ進む。

【００６８】ステップ５０２では、管理ポリシ１２６を参照し、前記問合せ中に指定されたアプリケーションの名称と一致するＡＰ名のレコードから更新指示の内容を読み出して、そのアプリケーションの更新指示が有るかどうかを調べ、更新指示の内容が「有」であり更新指示の有ることを示している場合にはステップ５０３へ進む。

【００６９】図６は本実施形態の管理ポリシ１２６の一例を示す図である。図６に示す様に本実施形態の管理ポリシ１２６は、最新の管理ポリシの取得先のＵＲＬを示す管理ポリシ取得先ＵＲＬと、管理ポリシ１２６が前回更新された日付を示す更新日付と、セキュリティチェック処理部１２４によりチェックが行われるアプリケーション処理の名称を示すＡＰ名の項目と、そのアプリケーションの更新が指示されているかどうかを示す更新指示と、そのアプリケーション処理を実行することが許可された期限を示す有効期限と、そのアプリケーション処理による携帯情報端末１００内の情報へのアクセスが許可されているかどうかを示す情報アクセスの項目と、そのアプリケーション処理による外部への通信処理が許可されているかどうかを示す通信の項目を有している。

【００７０】ステップ５０３では、ユーザＡＰ配布処理

13

装置３００へアクセスし、前記問合せの行われたアプリケーションの最新バージョンをユーザＡＰ配布処理装置３００から取得してユーザＡＰ１１４の更新処理を行い、管理ポリシ１２６中の前記レコードの更新指示の内容を「無」に変更する。

【００７１】ステップ５０４では、管理ポリシ１２６を参照し、前記問合せ中に指定されたアプリケーションの名称と一致するＡＰ名のレコードから有効期限を読み出す。

【００７２】ステップ５０５では、管理ポリシ１２６から読み出した有効期限と現在の日付とを比較し、現在の日付が前記有効期限内であり前記問合せの行われたアプリケーションが有効である場合にはステップ５０６へ進み、そのアプリケーション処理の実行が許可されていることを示す問合せ結果を、バックエンドＯＳ１２１、マルチＯＳ構成部１３０及びフロントエンドＯＳ１１１を経由してセキュリティエージェント１１２に送る。

【００７３】またステップ５０５で管理ポリシ１２６の有効期限と現在の日付とを比較した結果、現在の日付が前記有効期限を経過しており、前記問合せの行われたアプリケーションが有効ではない場合にはステップ５０７へ進み、そのアプリケーション処理の実行が許可されていないことを示す問合せ結果を、バックエンドＯＳ１２１、マルチＯＳ構成部１３０及びフロントエンドＯＳ１１１を経由してセキュリティエージェント１１２に送る。

【００７４】ステップ４０３でセキュリティエージェント１１２は、セキュリティチェック処理部１２４から返された問合せ結果を参照し、そのアプリケーション処理の実行が許可されていることを示す問合せ結果を受け取っている場合にはステップ４０４へ進み、そうでない場合には実行が許可されていないことを示すメッセージを出力装置１０４へ出力する。

【００７５】ステップ４０４では、前記アプリケーション処理の起動要求をフロントエンドＯＳ１１１に対して行ってそのアプリケーションを起動し、その起動されたアプリケーションのプロセスを識別する為の識別情報であるプロセスＩＤをフロントエンドＯＳ１１１から取得する。

【００７６】ステップ４０５では、フロントエンドＯＳ１１１から前記取得したプロセスＩＤと前記起動要求の行われたアプリケーションの名称を対応付けてメモリ１０２内に格納する。

【００７７】一方、ステップ４０１でアプリケーションの処理要求の内容を調べた結果、その処理要求がアプリケーション処理の起動要求ではない場合にはステップ４０６へ進む。

【００７８】ステップ４０６では、携帯情報端末１００上で行われたアプリケーションの処理要求の内容が携帯情報端末１００内のユーザデータ領域１５０に格納された住所録データや予定表データ等の情報へのアクセスであるかどうかを調べ、前記情報へのアクセスである場合にはステップ４０７へ進む。

14

【００７９】ステップ４０７では、前記処理要求を行ったアプリケーション処理のプロセスＩＤを取得し、メモリ１０２内に前記格納したプロセスＩＤとアプリケーション名称の情報から、そのプロセスＩＤに対応するアプリケーションの名称を読み出す。

【００８０】ステップ４０８では、前記読み出したアプリケーションの名称を指定し、そのアプリケーション処理による携帯情報端末１００内の情報へのアクセスが許可されているかどうかの問合せを、フロントエンドＯＳ１１１、マルチＯＳ構成部１３０及びバックエンドＯＳ１２１を経由してセキュリティチェック処理部１２４に送る。

【００８１】ステップ５０１でセキュリティチェック処理部１２４は、セキュリティエージェント１１２からの問合せの内容を調べ、その問合せ内容がアプリケーション処理の実行が許可されているかどうかの問合せではない場合にはステップ５０８へ進む。

【００８２】ステップ５０８では、セキュリティエージェント１１２からの問合せの内容を調べ、その問合せ内容がアプリケーション処理による携帯情報端末１００内の情報へのアクセスが許可されているかどうかの問合せである場合にはステップ５０９へ進む。

【００８３】ステップ５０９では、管理ポリシ１２６を参照し、前記問合せ中に指定されたアプリケーションの名称と一致するＡＰ名のレコードから情報アクセスの項目を読み出す。

【００８４】ステップ５１０では、管理ポリシ１２６から読み出した情報アクセスの項目内容を参照し、携帯情報端末１００内の情報へのアクセスが許可されている場合にはステップ５１１へ進み、そのアプリケーション処理による携帯情報端末１００内の情報へのアクセスが許可されていることを示す問合せ結果を、バックエンドＯＳ１２１、マルチＯＳ構成部１３０及びフロントエンドＯＳ１１１を経由してセキュリティエージェント１１２に送る。

【００８５】またステップ５１０で管理ポリシ１２６から読み出した情報アクセスの項目内容を参照した結果、携帯情報端末１００内の情報へのアクセスが許可されていない場合にはステップ５１２へ進み、そのアプリケーション処理による携帯情報端末１００内の情報へのアクセスが許可されていないことを示す問合せ結果を、バックエンドＯＳ１２１、マルチＯＳ構成部１３０及びフロントエンドＯＳ１１１を経由してセキュリティエージェント１１２に送る。

【００８６】ステップ４０９でセキュリティエージェント１１２は、セキュリティチェック処理部１２４から返された問合せ結果を参照し、そのアプリケーション処理

による携帯情報端末１００内の情報へのアクセスが許可されていることを示す問合せ結果を受け取っている場合にはステップ４１０へ進み、そうでない場合にはその情報へのアクセスが許可されていないことを示すメッセージを出力装置１０４へ出力する。

【００８７】ステップ４１０では、前記アプリケーション処理により行われた情報へのアクセス要求をフロントエンドＯＳ１１１に対して行ってその情報へのアクセスを実行し、その処理結果をフロントエンドＯＳ１１１から取得して当該アプリケーションに返す。

【００８８】一方、ステップ４０６でアプリケーションの処理要求の内容を調べた結果、その処理要求が携帯情報端末１００内の情報へのアクセス要求ではない場合にはステップ４１１へ進む。

【００８９】ステップ４１１では、携帯情報端末１００上で行われたアプリケーションの処理要求の内容が携帯情報端末１００外部への通信要求であるかどうかを調べ、前記外部への通信要求である場合にはステップ４１２へ進む。

【００９０】ステップ４１２では、前記処理要求を行ったアプリケーション処理のプロセスＩＤを取得し、メモリ１０２内に前記格納したプロセスＩＤとアプリケーション名称の情報から、そのプロセスＩＤに対応するアプリケーションの名称を読み出す。

【００９１】ステップ４１３では、前記読み出したアプリケーションの名称を指定し、そのアプリケーション処理による携帯情報端末１００外部への通信処理が許可されているかどうかの問合せを、フロントエンドＯＳ１１１、マルチＯＳ構成部１３０及びバックエンドＯＳ１２１を経由してセキュリティチェック処理部１２４に送る。

【００９２】ステップ５０１の処理の後、ステップ５０８でセキュリティチェック処理部１２４は、セキュリティエージェント１１２からの問合せの内容を調べ、その問合せ内容がアプリケーション処理による携帯情報端末１００内の情報へのアクセスが許可されているかどうかの問合せではない場合にはステップ５１３へ進む。

【００９３】ステップ５１３では、セキュリティエージェント１１２からの問合せの内容を調べ、その問合せ内容がアプリケーション処理による携帯情報端末１００外部への通信処理が許可されているかどうかの問合せである場合にはステップ５１４へ進む。

【００９４】ステップ５１４では、管理ポリシ１２６を参照し、前記問合せ中に指定されたアプリケーションの名称と一致するＡＰ名のレコードから通信の項目を読み出す。

【００９５】ステップ５１５では、管理ポリシ１２６から読み出した通信の項目内容を参照し、携帯情報端末１００外部への通信処理が許可されている場合にはステップ５１６へ進み、そのアプリケーション処理による携帯

情報端末１００外部への通信処理が許可されていることを示す問合せ結果を、バックエンドＯＳ１２１、マルチＯＳ構成部１３０及びフロントエンドＯＳ１１１を経由してセキュリティエージェント１１２に送る。

【００９６】またステップ５１５で管理ポリシ１２６から読み出した通信の項目内容を参照した結果、携帯情報端末１００外部への通信処理が許可されていない場合にはステップ５１７へ進み、そのアプリケーション処理による携帯情報端末１００外部への通信処理が許可されていないことを示す問合せ結果を、バックエンドＯＳ１２１、マルチＯＳ構成部１３０及びフロントエンドＯＳ１１１を経由してセキュリティエージェント１１２に送る。

【００９７】ステップ４１４でセキュリティエージェント１１２は、セキュリティチェック処理部１２４から返された問合せ結果を参照し、そのアプリケーション処理による携帯情報端末１００外部への通信処理が許可されていることを示す問合せ結果を受け取っている場合にはステップ４１５へ進み、そうでない場合には外部への通信処理が許可されていないことを示すメッセージを出力装置１０４へ出力する。

【００９８】ステップ４１５では、前記アプリケーション処理により行われた外部への通信要求をフロントエンドＯＳ１１１に対して行って外部への通信処理を実行し、その処理結果をフロントエンドＯＳ１１１から取得して当該アプリケーションに返す。

【００９９】前記の様に本実施形態の携帯情報端末１００では、携帯情報端末１００上で行われたアプリケーションの処理要求をセキュリティエージェント１１２で受け取り、その処理要求が許可されているかどうかを管理ポリシ１２６に従ってセキュリティチェック処理部１２４で判定し、その判定結果に応じてアプリケーション処理を実行することにより携帯情報端末１００でセキュリティ機能を提供しているので、管理ポリシ１２６にサービス事業者とは異なる基準でアプリケーションのアクセス可否の情報を設定することで、利用者である企業側の業務アプリケーションに適したセキュリティ機能を持たせることができる。

【０１００】なお本実施形態では、アプリケーションの有効期限、携帯情報端末１００内の情報アクセス、外部への通信処理に対するセキュリティ機能について説明したが、アプリケーション処理のバージョン毎に異なる有効期限を設定したり、携帯情報端末１００内の住所録データや予定表データの情報毎に異なるアクセス可否データや、読み出し、書き込み、削除等のアクセス内容毎に異なる可否データを設定したり、通信先のＵＲＬ毎に異なる可否データを設定する等、他の項目に対するセキュリティ機能を追加しても良い。

【０１０１】また、このセキュリティチェック処理及び管理ポリシ１２６の管理をバックエンドＯＳ１２１の制

御下で行う様にすることにより、フロントエンドＯＳ１１１が管理ポリシ１２６に直接アクセスすることがなくなるので、最新のフロントエンドＯＳ１１１に新たなセキュリティホールが発見された場合であっても、そのセキュリティホールによる管理ポリシ１２６への不正なアクセスを防止し、高いセキュリティを維持することができる。更に、フロントエンドＯＳ領域１１０とバックエンドＯＳ領域１２０とを異なる仮想メモリ空間とすることにより、フロントエンドＯＳ１１１からバックエンドＯＳ領域１２０へ直接アクセスする処理を禁止すれば、更に高いセキュリティを提供することが可能である。

【０１０２】更に本実施形態の携帯情報端末１００では、業務内容の変化に応じて業務用アプリケーションの機能を変更した場合に管理処理装置２００内の管理ポリシを変更しておき、管理ポリシアップデータ１２５により、管理処理装置２００内の管理ポリシの内容に従って携帯情報端末１００内の管理ポリシ１２６を更新することで、携帯情報端末１００の管理ポリシ１２６をリモートメンテナンスすることができる。

【０１０３】図７は本実施形態の管理ポリシアップデータ１２５の処理手順を示すフローチャートである。図７に示す様に本実施形態の管理ポリシアップデータ１２５は、管理処理装置２００内に格納された管理ポリシの内容に従って携帯情報端末１００内の管理ポリシ１２６を更新する処理を行う。

【０１０４】ステップ７０１で携帯情報端末１００の管理ポリシアップデータ１２５は、前回の処理からの所定時間の経過や利用者から特定のキーが押された場合等、管理ポリシ１２６の更新処理を開始する所定の条件が満たされたかどうかを調べ、前記条件が満たされている場合にはステップ７０２へ進む。

【０１０５】ステップ７０２では、携帯情報端末１００に格納されている管理ポリシ１２６を参照し、最新の管理ポリシの取得先のＵＲＬを示す管理ポリシ取得先ＵＲＬと管理ポリシ１２６が前回更新された日付を示す更新日付を読み出す。

【０１０６】ステップ７０３で管理ポリシアップデータ１２５は、前記読み出した管理ポリシ取得先ＵＲＬに示された管理処理装置２００のアドレスにアクセスし、管理処理装置２００に格納されている管理ポリシの更新情報の送信を管理処理装置２００に要求する。

【０１０７】管理処理装置２００は、管理ポリシの更新情報の取得要求を携帯情報端末１００から受信すると、管理処理装置２００内に格納されている管理ポリシが前回更新された日付を示す更新日付を読み出し、携帯情報端末１００へ送信する。

【０１０８】携帯情報端末１００の管理ポリシアップデータ１２５は、管理処理装置２００からフロントエンドＯＳ更新情報を受信するとステップ７０４に進み、管理ポリシ１２６から読み出した更新日付と、管理処理装置

２００から受信した更新日付とを比較し、携帯情報端末１００に格納されている管理ポリシ１２６の更新日付の方が古い場合には、管理ポリシ１２６の更新処理が必要であるものとしてステップ７０５へ進む。

【０１０９】ステップ７０５では、バックエンドＯＳ１２１を介してセキュリティチェック処理部１２４に処理の一時停止指示を送り、セキュリティチェック処理部１２４に処理の一時停止を指示する。

【０１１０】セキュリティチェック処理部１２４は、処理の一時停止指示を管理ポリシアップデータ１２５から受け取ると、現在処理中のセキュリティチェック処理を終了させた後、処理再開指示を待つ待ち状態に入る。

【０１１１】ステップ７０６で管理ポリシアップデータ１２５は、前記読み出した管理ポリシ取得先ＵＲＬに示された管理処理装置２００のアドレスにアクセスし、最新の管理ポリシデータの送信を管理処理装置２００に要求する。

【０１１２】ステップ７０７で管理ポリシアップデータ１２５は、管理処理装置２００から送信された管理ポリシデータを受信し、その管理ポリシデータを用いて、管理ポリシ１２６を最新の状態に更新する。この際、更新された管理ポリシ１２６に示されているＡＰ名とフロントエンドＯＳ領域１１０に格納されているユーザＡＰ１１４の名称とを比較し、更新された管理ポリシ１２６内に、携帯情報端末１００に格納されていない最新のユーザＡＰの情報が含まれている場合には、ユーザＡＰ配布処理装置３００へアクセスし、前記最新のユーザＡＰをダウンロードしてフロントエンドＯＳ領域１１０のユーザＡＰ１１４の更新を行っても良い。また、更新された管理ポリシ１２６内にアプリケーションの更新指示が有る場合には、そのアプリケーションの更新処理をここで行っても良い。

【０１１３】ステップ７０８では、バックエンドＯＳ１２１を介してセキュリティチェック処理部１２４に処理の再開指示を送り、セキュリティチェック処理部１２４に処理の再開を指示する。

【０１１４】セキュリティチェック処理部１２４は、処理の再開指示を管理ポリシアップデータ１２５から受け取ると、更新された管理ポリシ１２６を使用するセキュリティチェック処理を行える状態となる。

【０１１５】前記の様に本実施形態の携帯情報端末１００では、業務内容の変化に応じて業務用アプリケーションの機能を変更した場合に管理処理装置２００内の管理ポリシを変更しておくことにより、携帯情報端末１００内のユーザＡＰ１１４や管理ポリシ１２６のリモートメンテナンスを行うことが可能である。

【０１１６】以上説明した様に本実施形態の携帯情報端末によれば、フロントエンドＯＳの更新が必要であると判定された場合にバックエンドＯＳの制御下でフロントエンドＯＳの更新を行うので、携帯情報端末のＯＳの更

19

新を効率良く行うことが可能である。

【０１１７】また本実施形態の携帯情報端末によれば、管理ポリシに従って許可されたアプリケーションの処理要求を実行するので、携帯情報端末で利用者独自の基準に基づいたセキュリティ機能を実現することが可能である。

【０１１８】また本実施形態の携帯情報端末によれば、管理処理装置内に格納された管理ポリシの内容に従って携帯情報端末内の管理ポリシを更新するので、携帯情報端末内のセキュリティ機能をリモートメンテナンスすることが可能である。

【０１１９】

【発明の効果】本発明によればフロントエンドＯＳの更新が必要であると判定された場合にバックエンドＯＳの制御下でフロントエンドＯＳの更新を行うので、情報処理装置のＯＳの更新を効率良く行うことが可能である。

【図面の簡単な説明】

【図１】本実施形態の携帯情報端末マルチＯＳシステムの概略構成を示す図である。

【図２】本実施形態のフロントエンドＯＳアップデータ１２２の処理手順を示すフローチャートである。

【図３】本実施形態の更新情報管理テーブル１４２の一例を示す図である。

20

*【図４】本実施形態のセキュリティエージェント１１２の処理手順を示すフローチャートである。

【図５】本実施形態のセキュリティチェック処理部１２４の処理手順を示すフローチャートである。

【図６】本実施形態の管理ポリシ１２６の一例を示す図である。

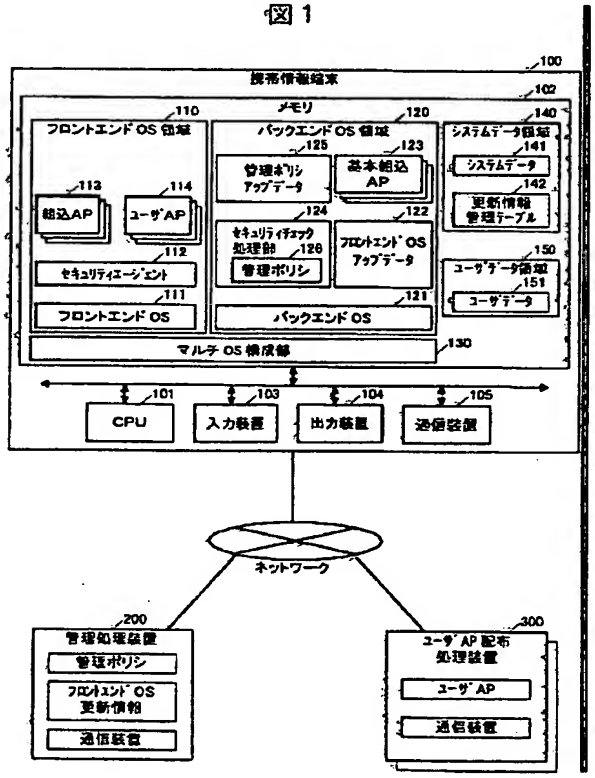
【図７】本実施形態の管理ポリシアップデータ１２５の処理手順を示すフローチャートである。

【符号の説明】

１００…携帯情報端末、２００…管理処理装置、３００…ユーザＡＰ配布処理装置、１０１…ＣＰＵ、１０２…メモリ、１０３…入力装置、１０４…出力装置、１０５…通信装置、１１０…フロントエンドＯＳ領域、１２０…バックエンドＯＳ領域、１２６…管理ポリシ、１４０…システムデータ領域、１４１…システムデータ、１４２…更新情報管理テーブル、１５０…ユーザデータ領域、１５１…ユーザデータ、１１１…フロントエンドＯＳ、１１２…セキュリティエージェント、１１３…組込ＡＰ、１１４…ユーザＡＰ、１２１…バックエンドＯＳ、１２２…フロントエンドＯＳアップデータ、１２３…基本組込ＡＰ、１２４…セキュリティチェック処理部、１２５…管理ポリシアップデータ、１３０…マルチＯＳ構成部。

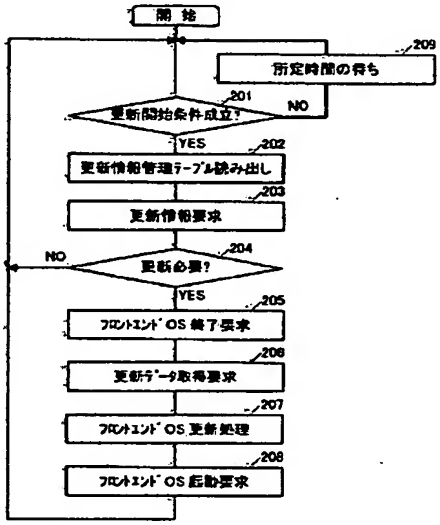
【図１】

図１



【図２】

図２



【図３】

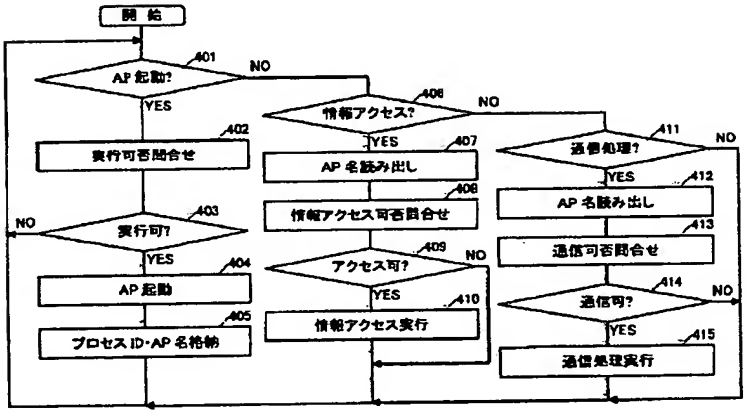
図３

名称	バージョン	更新日付	格納ｱﾄﾞﾚｽ	長さ	更新情報取得先 URL
ﾌﾛﾝﾄｴﾝﾄﾞ OS	3.02	2001.2.1	00000	1024	http://www.feos…
組込 AP 1	1.01	2001.7.1	00100	256	http://www.ap1…
組込 AP 2	2.31	2001.3.11	00200	512	http://www.ap2…
：	：	：	：	：	

142

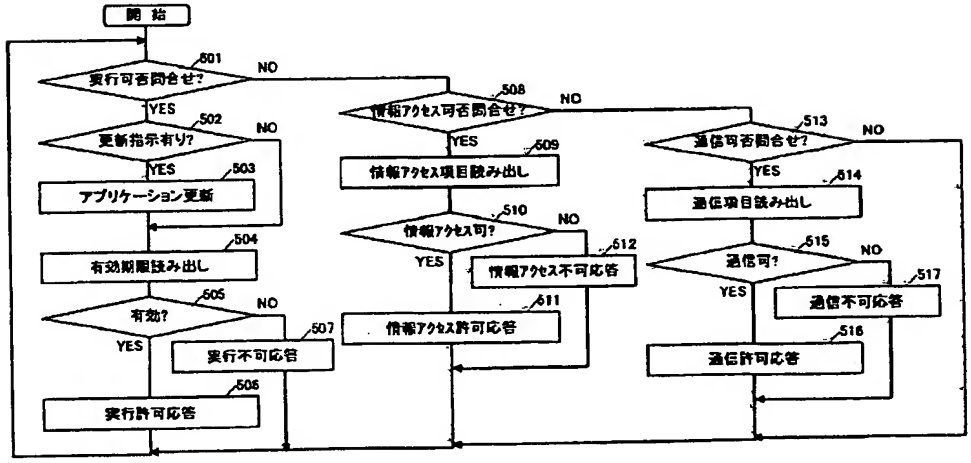
【図４】

図４



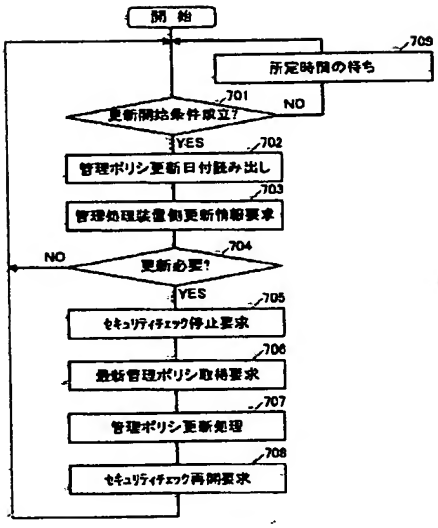
【図５】

図５



【図７】

図７



【図６】

図６

126

管理ポリシ 管理ポリシ取得先 http://www.policy.***, 更新日付 2001.10.1				
AP名	更新指示	有効期限	情報アクセス	通信
AP1	無	2001.12.31	可	不可
AP2	有	2002.3.31	不可	可
:	:	:	:	:

フロントページの続き

(72)発明者　新井　利明
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

Ｆターム(参考)　5B076 AA02 AA13 EB02 FB00